aurigin

Document Summary

New Search Help

Preview Claims
Preview Full Text
Preview Full Image

Email Link:

Document ID:	JP 09-269930 A2
Title:	METHOD AND DEVICE FOR PREVENTING VIRUS OF NETWORK SYSTEM
Assignee:	HITACHI LTD
Inventor:	KONDO TAKESHI SHIGESA HIDEHIKO
US Class:	
Int'l Class:	G06F 15/00 A; G06F 09/06 B; G06F 13/00 B
Issue Date:	10/14/1997
Filing Date:	04/03/1996

Abstract:

PROBLEM TO BE SOLVED: To construct a computer network system whose resistance against a computer virus is strong.

SOLUTION: A frame repeater 100 has a means 202 for checking whether the computer virus is contained in a repeating frame or not and a warning message frame generation means 203 started at the time of detecting a virus frame. A means for receiving and displaying a warning message is provided in a computer connected to a network. Since the invasion of the computer virus, the diffusion and the influence range of damage can be set to minimum, the computer network system of high safety and reliability, which is provided with a resistance means for computer virus can be provided.

(C)1997,JPO

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平9－269930
(43)公開日　平成９年(1997)10月14日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	15/00	３３０		Ｇ０６Ｆ	15/00	３３０Ａ
	9/06	５５０			9/06	５５０Ｚ
	13/00	３５１			13/00	３５１Ｚ

審査請求 未請求　請求項の数26　ＯＬ　（全 23 頁）

(21)出願番号　特願平8－81184

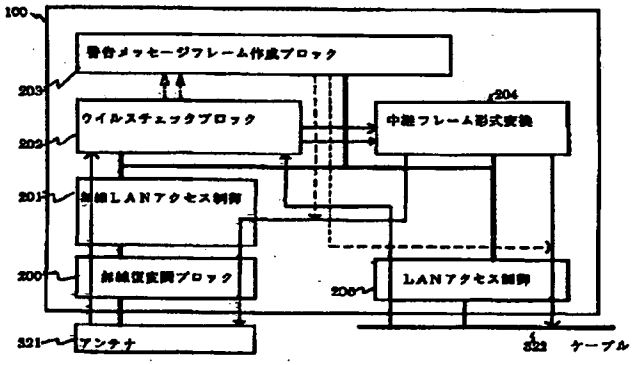
(22)出願日　平成８年(1996)４月３日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　近藤　毅
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内
(72)発明者　重左　秀彦
神奈川県海老名市下今泉810番地株式会社日立製作所オフィスシステム事業部内
(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　ネットワークシステムの防疫方法及びその装置

(57)【要約】
【課題】コンピュータウイルスへの耐性が強いコンピュータネットワークシステムを構築する。
【解決手段】フレーム中継装置１００に中継フレームにコンピュータウイルスが含まれていないかどうかをチェックする手段２０２とウイルスフレーム検出時に起動される警告メッセージフレーム作成手段２０３とを備える。前記警告メッセージを受信し表示する手段をネットワークに接続されたコンピュータに設ける。コンピュータウイルスの侵入やその拡散及びその被害の影響範囲を最小限にすることができるのでコンピュータウイルスへの対抗手段を備えた安全性および信頼性の高いコンピュータネットワークシステムを提供できる。

図 2



1

【特許請求の範囲】

【請求項1】多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、

前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェックステップと、

当該ウイルスチェックステップにおいて、ウイルスが含まれると判断したデータの前記伝送路上の通過を阻止するフィルタリングステップと、

前記ウイルスチェックステップで前記伝送路を流れるデータ中にウイルスを検出した場合、警告メッセージを前記ネットワークシステム上に送出する警告通報ステップと、

当該警告通報ステップによる警告メッセージを受信し、当該受信した警告メッセージに基づいて、ウイルスが検出されたことをユーザに知らせるための情報を前記コンピュータ上に表示する提示ステップと、

前記ウイルスのフィルタリングステップにより阻止された前記データが受信先に到達しないことによる影響を処理する後処理ステップとを有することを特徴とするネットワークシステムの防疫方法。

【請求項2】ウイルスチェックステップで、データ圧縮または暗号の少なくとの一方により変形したコンピュータウイルスを識別することを特徴とする請求項1記載のネットワークシステムの防疫方法。

【請求項3】多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、

前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェックステップと、

前記ウイルスチェックステップで前記伝送路を流れるデータ中にウイルスを検出したことにより、当該データに関連するコンピュータに警告メッセージを送信する警告通報ステップと、

前記警告通報ステップにより送られた前記警告メッセージを受信したことを契機に、検出されたウイルスに対抗する処理を実行するウイルス駆除ステップとを有することを特徴とするネットワークシステムの防疫方法。

【請求項4】多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、

前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かを推定するウイルス推定ステップと、

前記ウイルス推定ステップにおいて、ウイルスが含まれていると推定した場合、注意メッセージを前記データの受信コンピュータに送付する注意通報ステップと、

前記注意通報ステップによる注意メッセージを受信し、これに基づいて当該受信データを含むデータファイルに実際にウイルスが存在しているかどうかの検査を依頼する検査依頼ステップと前記検査依頼を受けて検査を実行する検査ステップと前記検査ステップにおける検査結果を依頼者に報告する報告ステップとを有することを特徴とするネットワークシステムの防疫方法。

2

【請求項5】コンピュータネットワークシステムは、複数の異なる伝送路と、当該伝送路を中継する中継装置を備え、

検査ステップにおける検査でコンピュータウイルスが入っているとされたデータファイルから当該コンピュータウイルスの識別情報を抽出するステップと、

当該識別情報を前記中継装置に配布するステップと、

前記中継装置において、前記ステップにより送られたウイルス識別情報を登録し、これに基づいてウイスルフィルタリングを実行するステップとを有したことを特徴とする請求項4記載のネットワークシステムの防疫方法。

【請求項6】中継装置は、新規ウイルス識別情報を定期的に隣接するネットワーク中継装置と交換する機能を備えたことを特徴とする請求項5記載のネットワークシステムの防疫方法。

【請求項7】伝送路に当該伝送路上のデータをモニタする監視装置を接続し、検査ステップにおける検査でコンピュータウイルスが入っているとされたデータファイルから当該コンピュータウイルスの識別情報を抽出するステップと、

当該識別情報を前記監視装置に配布するステップと、

前記監視装置において、前記ステップにより送られたウイルス識別情報を登録し、これに基づいてウイルスチェックを実行するステップとを有したことを特徴とする請求項4記載のネットワークシステムの防疫方法。

【請求項8】多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、

前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェック手段と、

当該ウイルスチェック手段にて、ウイルスが含まれると判断したデータの前記伝送路上の通過を阻止するフィルタリング手段と、

前記ウイルスチェック手段で前記伝送路を流れるデータ中にウイルスを検出した場合、警告メッセージを前記ネットワークシステム上に送出する警告通報手段と、

当該警告通報手段からの警告メッセージを受信し、当該受信した警告メッセージに基づいて、ウイルスが検出されたことをユーザに知らせるための情報を前記コンピュータ上に表示する提示手段と、

前記ウイルスのフィルタリング手段により阻止された前記データが受信先に到達しないことによる影響を処理する後処理手段とを具備して成るネットワークシステムの防疫装置。

【請求項9】コンピュータネットワークシステムは複数の異なる伝送路と、当該伝送路を中継する中継装置を備え、当該中継装置に、ウイルスチェック手段とフィルタ

リング手段を具備し、前記中継装置のフィルタリング手段はウイルスが含まれたデータを中継しないことによりデータの伝送路上の通過を阻止する請求項8記載のネットワークシステムの防疫装置。

【請求項10】コンピュータは、当該コンピュータ上で動作するネットワークを使用したアプリケーションプログラムが異常終了したとき、ネットワークの故障によるものか、あるいはウイルス侵入防止によるものかをきり分ける手段を備えたことを特徴とする請求項8記載のネットワークシステムの防疫装置。

【請求項11】中継装置は、特定の情報を制御ヘッダに付加した伝送フレームをウイルスチェック結果にかかわらず中継することを特徴とする請求項9記載のネットワークシステムの防疫装置。

【請求項12】ウイルスチェック手段は、データ圧縮ないしは暗号により変形したコンピュータウイルスを識別する手段を備えて成る請求項8記載のネットワークシステムの防疫装置。

【請求項13】多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、
前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェック手段と、
前記ウイルスチェック手段で前記伝送路を流れるデータ中にウイルスを検出したら、当該データに関連するコンピュータに警告メッセージを送信する警告通報手段と、
前記警告通報手段から送られた前記警告メッセージを受信したことを契機に検出されたウイルスに対抗する処理を実行するウイルス駆除手段とを有することを特徴とするネットワークシステムの防疫装置。

【請求項14】伝送路に、当該伝送路上のデータをモニタする監視装置を接続し、当該監視装置にウイルスチェック手段と、警告通報手段とを備えたことを特徴とする請求項13記載のネットワークシステムの防疫装置。

【請求項15】コンピュータは、警告通報手段からの警報メッセージを受信する手段と、当該メッセージに基づき当該コンピュータのユーザにウイルス侵入警告を表示する手段とを備えたことを特徴とする請求項13記載のネットワークシステムの防疫装置。

【請求項16】監視装置は、ワクチンプログラムを格納する手段と、検出されたウイルスに対応するワクチンプログラムを関連するコンピュータに送付する手段とを備えたことを特徴とする請求項14記載のネットワークシステムの防疫装置。

【請求項17】伝送路に、限定された範囲のネットワークをモニタするネットワーク監視装置を複数接続し、複数のモーバイルコンピュータも接続したネットワークシステムにおいて、予め定めた特定範囲に所在する前記ネットワーク監視装置にウイルス検出メッセージを配布する手段を備えたことを特徴とする請求項13記載のネットワークシステムの防疫装置。

【請求項18】無線ネットワークに接続する複数のモーバイルコンピュータをネットワークシステムの構成要素として含み、当該モーバイルコンピュータでのウイルス警告メッセージの表示において、検出されたウイルスに対応するワクチンプログラムの実行が完了するまで電源を切らないことと、他のセルに移動しないようにとの注意事項をユーザに通知する手段を備えたことを特徴とする請求項13記載のネットワークシステムの防疫装置。

【請求項19】コンピュータに、ウイルスチェック手段と、警告通報手段とを備え、更に警告メッセージからウイルスを送り出したコンピュータの識別情報を認識してこれを記憶する記憶手段と、前記記憶手段に登録されたコンピュータとの通信を控えさせる手段と、前記記憶手段に登録されたウイルス保有コンピュータのウイルス駆除完了通知により前記記憶手段から当該コンピュータを削除する手段とを備えたことを特徴とする請求項13記載のネットワークシステムの防疫装置。

【請求項20】コンピュータは、モーバイルコンピュータであり、ウイルスを送信したコンピュータの位置情報を警告メッセージから認識する手段と、ウイルスを保有したコンピュータの所在を提示する手段とを備えたことを特徴とする請求項19記載のネットワークシステムの防疫装置。

【請求項21】ウイルス送信コンピュータの登録手段と、ウイルス送信コンピュータ登録の解除手段と、前記手段により登録を解除されたことを通報する手段とを備えたことを特徴とする請求項14記載のネットワークシステムの防疫装置。

【請求項22】多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、
前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かを推定するウイルス推定手段と、
前記ウイルス推定ステップにおいて、ウイルスが含まれていると推定した場合、注意メッセージを前記データの受信コンピュータに送付する注意通報手段と、
前記注意通報ステップによる注意メッセージを受信し、これに基づいて当該受信データを含むデータファイルに実際にウイルスが存在しているかどうかの検査を依頼する検査依頼手段と、
前記検査依頼を受けて検査を実行する検査手段と、
前記検査ステップにおける検査結果を依頼者に報告する報告手段とを有することを特徴とするネットワークシステムの防疫装置。

【請求項23】ウイルス推定手段にて、ウイルスが含まれると判断したデータの前記伝送路上の通過を阻止するフィルタリング手段を備えて成る請求項22記載のネットワークシステムの防疫装置。

【請求項24】検査依頼手段による検査依頼中のデータファイルのアクセスを禁止する手段を備えたことを特徴

5

とする請求項２２記載のネットワークシステムの防疫装置。

【請求項２５】他のコンピュータからの検査依頼受付機能と、当該コンピュータに対する前記検査結果を報告する機能とを備えたことを特徴とする請求項２２記載のネットワークシステムの防疫装置。

【請求項２６】伝送路に当該伝送路上のデータをモニタする監視装置を接続し、コンピュータに新規ウイルスにたいするワクチンプログラムの作成手段を備え、
前記監視装置に対して、前記新規ウイルスに対するワクチンプログラムを配布する手段を備えたことを特徴とする請求項２２記載のネットワークシステムの防疫装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータネットワークシステムの安全性を高める発明であり、特に安全性を保証しにくいモーバイルコンピュータを接続した無線ネットワークから、安全性や信頼性要求される基幹ネットワークにコンピュータウイルスやコンピュータワームが進入することで、基幹ネットワーク上のコンピュータにシステムダウン等の悪影響を与える事を抑止する発明である。

【０００２】また、たとえ、当該ネットワーク上のコンピュータがウイルスに感染したとしても、そこからウイルス感染を拡大させないことで、コンピュータウイルスによって被害をうけるコンピュータをなるべく少なく抑えるコンピュータネットワークシステムに関する発明でもある。

【０００３】また、ウイルスにより汚染されたコンピュータにたいしてウイルスワクチンソフトをすばやく汚染コンピュータに投与実施することによりウイルスをすばやく駆除することにより、ウイルスにたいする耐性を強化したコンピュータネットワークシステムに関する発明でもある。

【０００４】

【従来の技術】パーソナルコンピュータをパソコン通信用のネットワークやインターネットに接続し、それらのネットワークのサーバに格納されたファイルをダウンロードすることが広く普及している。前述したファイルにコンピュータウイルスが潜んでいるとそのファイルの実行時等に当該コンピュータ内に寄生する。寄生したコンピュータウイルスは、潜伏したり、再感染のための自己複製を作る。そして、コンピュータウイルスは、ある条件が整うとソフトウェアを破壊するなどの様々な悪影響を与える。これを除去するためにコンピュータウイルスのワクチンソフトを定期的に起動して感染していないかチェックすることで、コンピュータウイルスを除去している。

【０００５】特に、インターネットでは、情報提供者としてのビジネスの利用や各種の情報を入手できるメリット等があるため、企業において、従来の企業内ネットワークをインターネット接続する例が増えている。このような企業内ネットワークでは、信頼性が必要であり、パスワードによる認証等により、各種ネットワーク機器へのアクセスを監理することで信頼性を保っていた。例えば、このような技術に関する発明が「ローカルエリア・ネットワークのセキュリティ方法及びそのシステム」として特開平７－１３１４５１で公開されている。

【０００６】セキュリティを保ちながら、インターネット接続する方法として、ファイヤーウオール等でアクセス者を限定する方法があるが、コンピュータウイルスにたいする対策は、上述したように、個々の計算機で上述した方法で対応しており、システム的な対応はなされていない。

【０００７】また、多数のコンピュータが接続するインターネットは、セキュリティに関しては非常に低いレベルにある。このため、悪意あるハッカー達により、今までにない新しいコンピュータウイルスが開発され、これが流行する恐れもある。それは、このような新しいウイルスに対応したワクチンが開発される迄時間がかかることともしこのような新しいウイルスの潜伏期間が長いと新しいウイルスの検出までに時間がかかることによる。このような新しいコンピュータウイルスに対抗するため、あるコンピュータでウイルスによる異常を監視しておき、異常を検出したらそのウイルスの識別子を特定し、その特定情報を各コンピュータに配布するという方法が「コンピュータを生態免疫システム的に強化する方法」としてＪeffrey　O.kephartが:To appear in Artificial Life ＩＶ,R.Brooks and P.Meas,eds.,ＭＩＴ　Press,１９９４で発表している。

【０００８】

【発明が解決しようとする課題】上記従来技術によると、以下のような課題がある。

【０００９】課題１：ウイルスが当該マシンに侵入したとき、ウイルススキャンプログラムやワクチンプログラムを起動するまでの間にネットワークを介して他のマシンに二次感染する。即ち、ウイルスの蔓延を防ぐ事ができない。

【００１０】課題２：例えばファイルをダウンロードするたびにウイルスチェックのためスキャンプログラムやワクチンプログラムを起動したのでは、マシンにオーバーヘッドがかかる。また、ファイルの起動のたびに前記プログラムをいちいち起動するのは、ユーザにとって煩わしい作業である。

【００１１】課題３：また、いつワクチンを起動すれば適切かわからないため、通常、定期的にウイルスチェックプログラムを実行する。このような場合、ウイルスに感染していなくても、ウイルスチェックプログラムによるメモリチェック等の処理負荷がコンピュータにかかる。

【００１２】課題４：更に、悪意を持った者がウイルスをばらまくために、ウイルス入りのファイルをだれでもアクセスできるサーバにアップロードするということも防げない。

【００１３】等である。

【００１４】

【課題を解決するための手段】上記課題は、以下の次の手段、すなわち、

手段１：ウイルスフィルタ機能を備えたネットワーク上を流れるデータの中継手段または、

手段２：ウイルス検出メッセージ発信機能を備えた中継装置と前記メッセージを表示する機能を備えたコンピュータ装置

のいずれかによって原理的に解決できる。

【００１５】すなわち、本発明の特徴とするところは、多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェックステップと、当該ウイルスチェックステップにおいて、ウイルスが含まれると判断したデータの前記伝送路上の通過を阻止するフィルタリングステップと、前記ウイルスチェックステップで前記伝送路を流れるデータ中にウイルスを検出した場合、警告メッセージを前記ネットワークシステム上に送出する警告通報ステップと、当該警告通報ステップによる警告メッセージを受信し、当該受信した警告メッセージに基づいて、ウイルスが検出されたことをユーザに知らせるための情報を前記コンピュータ上に表示する提示ステップと、前記ウイルスのフィルタリングステップにより阻止された前記データが受信先に到達しないことによる影響を処理する後処理ステップとを有することにある。

【００１６】また、本発明の特徴とするところは、多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェックステップと、前記ウイルスチェックステップで前記伝送路を流れるデータ中にウイルスを検出したことにより、当該データに関連するコンピュータに警告メッセージを送信する警告通報ステップと、前記警告通報ステップにより送られた前記警告メッセージを受信したことを契機に、検出されたウイルスに対抗する処理を実行するウイルス駆除ステップとを有することにある。

【００１７】更に、本発明の特徴とするところは、多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かを推定するウイルス推定ステップと、前記ウイルス推定ステップにおいて、ウイルスが含まれていると推定した場合、注意メッセージを前記データの受信コンピュータに送付する注意通報ステップと、前記注意通報ステップによる注意メッセージを受信し、これに基づいて当該受信データを含むデータファイルに実際にウイルスが存在しているかどうかの検査を依頼する検査依頼ステップと、前記検査依頼を受けて検査を実行する検査ステップと、前記検査ステップにおける検査結果を依頼者に報告する報告ステップとを有することにある。

【００１８】更に、本発明の特徴とするところは、多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェック手段と、当該ウイルスチェック手段にて、ウイルスが含まれると判断したデータの前記伝送路上の通過を阻止するフィルタリング手段と、前記ウイルスチェック手段で前記伝送路を流れるデータ中にウイルスを検出した場合、警告メッセージを前記ネットワークシステム上に送出する警告通報手段と、当該警告通報手段からの警告メッセージを受信し、当該受信した警告メッセージに基づいて、ウイルスが検出されたことをユーザに知らせるための情報を前記コンピュータ上に表示する提示手段と、前記ウイルスのフィルタリング手段により阻止された前記データが受信先に到達しないことによる影響を処理する後処理手段とを具備して成るネットワークシステムの防疫装置にある。

【００１９】更に、本発明の特徴とするところは、多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かをチェックするウイルスチェック手段と、前記ウイルスチェック手段で前記伝送路を流れるデータ中にウイルスを検出したら、当該データ関連するコンピュータに警告メッセージを送信する警告通報手段と、前記警告通報手段から送られた前記警告メッセージを受信したことを契機に検出されたウイルスに対抗する処理を実行するウイルス駆除手段とを有することにある。

【００２０】更に、本発明の特徴とするところは、多数のコンピュータを伝送路を介して接続したコンピュータネットワークシステムにおいて、前記伝送路上を流れるデータにコンピュータウイルスが含まれているか否かを推定するウイルス推定手段と、前記ウイルス推定ステップにおいて、ウイルスが含まれていると推定した場合、注意メッセージを前記データの受信コンピュータに送付する注意通報手段と、前記注意通報ステップによる注意メッセージを受信し、これに基づいて当該受信データを含むデータファイルに実際にウイルスが存在しているかどうかの検査を依頼する検査依頼手段と、前記検査依頼を受けて検査を実行する検査手段と、前記検査ステップにおける検査結果を依頼者に報告する報告手段とを有することにある。

9

【００２１】上記のように構成すれば、ネットワーク上のコンピュータは、他のコンピュータとデータ通信することで、データファイルを自分のコンピュータのメモリ上にロードする。このようなネットワーク上でコンピュータは、ウイルス入りのファイルをアクセスし、これを実行したりするとウイルスに感染する。いま、中継装置を介して相互に接続するネットワークを考えれば、前述した手段１がウイルス入りのデータをフィルタするので、ウイルス入りのファイル等をリモートからアクセスしようとすると、必ず当該ファイルのデータ通信が失敗する事になる。結果として、ウイルスに汚染されたファイルはアクセスできなくなるので、ウイルスに感染する事はなくなる。よって、ワクチンソフトを定期的に起動しなくてもすむ。また、悪意を持ったユーザが、ウイルスをばらまこうとして、ウイルスの感染媒体であるファイルを、自由にアクセスできる公開されたファイルサーバに登録しようとしても、前記手段１によって、結果的にファイル転送が失敗する。これにより、ウイルス入りのファイルは当該ネットワークにおいて感染媒体としての役割を果たさなくなるため、ウイルスの拡散を防げる。

【００２２】また、手段２によれば、ウイルス検出メッセージを受信したコンピュータは、ウイルス入りのファイルをロードしようとした事がわかるため、その対応をなすことができる。例えば、ウイルスに寄生される前なら当該ファイルを削除したりできる。また、ワクチンプログラムを当該メッセージ受信のタイミングで実行する事ができ、その結果ウイルスの駆除が直ちに行える。

【００２３】

【発明の実施の形態】

実施例１

無線ネットワークから基幹ネットに接続されたコンピュータに侵入を企てているウイルスをネットワーク上の検知して、それをファイルタリングし侵入ターゲットとなったコンピュータシステムにたいして、警告を与えるネットワークシステムの実施例をこれから説明する。

【００２４】図１は、本発明の一実施例におけるシステム構成を表した図である。

【００２５】本システムは伝送路に光や電波などの電磁波を使用した無線ネットワークと伝送路にケーブルを使用した有線ネットワークとを接続したコンピュータネットワークシステムであり、以下に述べるコンポーネントから構成される。１００は、無線ブリッジ（以下ＷＢと略称する）であり、有線ネットワークと無線ネットワークとの接続装置である。無線ブリッジ１００は、有線ネットワークを流れるデータフレームを無線ネットワーク側に中継したり、またその逆に無線ネットワーク上を流れるデータフレームを有線ネットワーク上に中継したりする。

【００２６】１０１は、個人用の計算機システムである

10

パーソナルコンピュータ（以下ＰＣと略称する）である。ＰＣ１０１は、有線ネットワーク上に接続され、ネットワークに接続された他の計算機システムとデータ通信を行う。

【００２７】１０２は、ポータブルな計算機システムであるモーバイルコンピュータ（以下ＭＴと略称する）である。ＭＴ１０２は、無線送受信機を使用して無線ネットワークに接続し、ネットワークに接続された他の計算機システムとデータ通信を行う。例えば、ＰＣ１０１に電子メールや電子化されたファイルを蓄積しておき、ＭＴ１０２を離れた場所に持ち込み、その場で前述の電子メールを読んだり、電子ファイルの内容を更新したりする。

【００２８】１０３は、有線ネットワーク上を流れるデータの配送を制御するルータである。ルータ１０３は、複数のネットワークと接続し、パケット化されたデータ（単にパケットと呼ぶ）に記された配送アドレスに応じて、あるネットワーク上のパケットを他のネットワークに送る機能を持つ。

【００２９】１０４は、ＷＢ１００の無線機がカバーするエリアである無線Ｉａｎセルである。本セル内では、同一の周波数帯域が使用されるため、当該セル内に収容されているＭＴ１０２間で通信ができる。

【００３０】１０５は、ローカルエリアネットワーク（以下ＬＡＮと略称する）であり、先述したＰＣ１０１やＷＢ１００，ＭＴ１０２が複数台接続したルータ１０３によって仕切られた局地的なネットワークである。このローカルネットワーク１０５は、ＭＴ１０２とＷＢ１００から構成される無線ＬＡＮを含んでいる。

【００３１】１０６は、インターネットであり、前述したルータ１０３により相互接続されたコンピュータネットワークの集合体である。

【００３２】まず、本発明のネットワーク防疫機能をＷＢ１００に実装した例を説明する。

【００３３】図２で示すＷＢ１００内の各機能ブロックによってＭＴ１０２からＰＣ１０１へのウイルス進入防止機構が実現される。

【００３４】ＷＢ１００は、先述したように、有線ネットワーク上でのデータフレームを無線ネットワーク上に中継したり、またその逆方向の中継も行う。そのための機能ブロックが無線復変調ブロック２００、無線ＬＡＮアクセス制御２０１、中継フレーム変換２０４、及びＬＡＮアクセス制御２０５の各ブロックである。これらのフレーム中継機能ブロックに対して、ウイルスの進入をフィルタすることによりネットワークの安全性を高める機能ブロックが、ウイルスチェックブロック２０２と警告メッセージフレーム作成ブロック２０３である。無線ネットワーク側から基幹ネットワークである有線ネットワーク側に侵入しようとするコンピュータウイルスを例にして各ブロックの働きを説明する。

11

【００３５】まずアンテナ３２１でデータフレームの情報が乗せられた電波を受け取る。そして、無線復変調ブロック２００が受信電波信号からフレームを構成する信号を取り出し、そこから無線ＬＡＮアクセス制御２０１がデータフレームを再構築する。次に、受信したデータフレームの中に、コンピュータウイルスを構築するための情報が入っていないかどうかをウイルスチェックブロックが検査する。この結果、ウイルスを含まないフレームならば、次のブロックである中継フレーム形式変換２０４に送られる。中継フレーム形式変換２０４は、無線側と有線側のフレーム形式の変換する。そして、有線ＬＡＮ上のフレームに変換された後、ＬＡＮアクセス制御２０５に渡り、そこから有線ケーブル３２２上にフレーム信号が送出される。これに対して、ウイルスチェックブロック２０２で、ウイルスが含まれていると判定されたフレームは、中継フレーム変換２０４に渡さないので、有線ネットワーク側に流れず、ＷＢ１００ないで阻止される。このときウイルスチェックブロック２０２は、警告メッセージフレーム作成ブロック２０３に受信フレームでウイルスを検出した事を通知する。これを受けた警告メッセージ作成ブロック２０３は、ウイルス検出警告メッセージを作成し、ウイルス入りフレームの送り元とその宛先にたいして、前記メッセージを送るため、それぞれ、無線ＬＡＮアクセス制御２０１とＬＡＮアクセス制御２０５に警告メッセージを渡す。これを受けた各々の制御ブロックは、警告メッセージフレームをネットワーク上に送出する。

【００３６】次にＷＢ１００のハードウェア構造を図３を使って説明する。

【００３７】３００は、ＭＰＵでありＷＢ１００の処理ソフトウェアの実行ユニットである。ＲＡＭ３０１は、ＭＰＵ３００が書き換え可能な記憶装置である。ＲＯＭ３０２は、書き換え不可能な読みだし専用の記憶ユニットであり、ＷＢ１００の処理ソフトウェアが記憶されている。３０３は、ＬＡＮの標準規格であるＥｔｈｅｒＮｅｔの制御ＬＳＩであり、伝送ケーブル３２２で接続される有線ＬＡＮへのフレーム送信や有線ＬＡＮからのフレーム受信を処理するハードウェアユニットである。３１０は、ＭＰＵバスであり、ＲＡＭ３０１やＲＯＭ３０２等の記憶装置や３０３，３０４等の入出力制御ＬＳＩが接続されている。３０４は、無線ＬＡＮ側の入出力制御ＬＳＩであり、バス３１０のインタフェース機能と無線ＬＡＮに対するアクセス制御を行う機能とを備える。３０６は、復変調ＬＳＩで有り、フレームを構成する情報を搬送電波に乗せるための信号に変調したり、逆に、搬送電波に乗せられた信号からフレームを構成する情報を取り出す復調したりする機能を持つ。３０６は、ＲＦインタフェースＬＳＩであり、ＲＦユニット３０７の発信・受信等の制御を行う。３０７は、ＲＦユニットであり、使用帯域周波数の電波を送信したり、受信したりするユニットである。３２１はアンテナである。

12

【００３８】次に、図４を用いてＷＢ１００の処理ソフトウェアモジュール構成について説明する。

【００３９】４０４は、無線ＬＡＮドライバモジュールであり、無線ＬＡＮのアクセス制御ＬＳＩである３０７の制御用ソフトウェアである。これに対して、４０６は、ＥｔｈｅｒＮｅｔドライバであり、ＥｔｈｅｒＮｅｔ制御ＬＳＩ３０３用の制御用ソフトウェアである。４０３は、ＬＡＮドライバ共通制御で有り、無線ＬＡＮと有線ＬＡＮの制御においてフレーム送受信等の共通となる制御ロジックをまとめたソフトウェアモジュールである。４０２は、ブリッジ処理であり、フレーム形式の相互変換機能とフレーム中継機能、及び、フレームヘッダに記載されたアドレスによるフィルタリング機能を実現する。４０１は、ウイルスチェックモジュールであり、ブリッジ処理における中継フレームの情報フィールドを見て、そこにウイルスのコードが記載されていないかどうかをチェックし、ウイルス入りのフレームをフィルタリングする機能をもつ。４００は、セキュリティ管理モジュールであり、ウイルスフレームを検出した４０１から通知を受けた後、当該フレームの送り元と宛先のアドレスに対する警告メッセージを作成する機能をもつ。４０５は、通信プロトコル処理モジュールであり警告メッセージを受け取るＰＣ１０１やＭＴ１０２上のセキュリティ管理プロセスに対するメッセージの配送を保証する機能を持つ。

【００４０】次に、図４で示した各処理ソフトウェアモジュールがどのような処理ロジックによって総括されているかを図５のＷＢ処理フローで説明する。まずはじめのステップは、受信フレーム待ちであり（ステップ５０２）、無線・有線Ｌａｎの各ドライバ４０４，４０６からドライバ共通制御４０３を介して正当なフレーム受信の報告が対応するハードウェアユニットからブリッジ処理４０２にくるまで待つステップである。次に、ブリッジ処理部でのファイルタリングを行った後、ウイルスチェックモジュール４０１で受信フレームの検査を行う（ステップ５０４）。ステップ５０４でのチェックで当該フレームにウイルスが含まれていなければ、中継処理ステップ５１０に移り、もし、含まれているならば、警告メッセージ作成ステップ５０６に移る。ウイルスが含まれていた場合のフローから説明する。

【００４１】警告メッセージ作成ステップ５０６では、セキュリティ管理モジュール４００で、送り元と宛先に対する警告メッセージをウイルスチェック結果に応じてそれぞれ作成するステップである。次は、メッセージフレーム処理ステップであり、前記メッセージに通信プロトコルヘッダを付加してフレームを作成し、それぞれに対するフレーム送信要求をＬＡＮドライバ共通制御４０２に発行することを通信プロトコル処理４０５において実行する（ステップ５０８）。次にステップ５０２にお

いて当該フレームにウイルスを検出しなかった場合の処理フローについて説明する。このときは中継処理ステップとしてブリッジ処理モジュール４０２でフレームの変換をしてＬＡＮドライバ共通制御４０３に異なるサイドＬＡＮに送出するように送信要求を出す（ステップ５１０）。残りの処理ステップは、フレーム送信であり、要求されたフレームを指定された側のＬＡＮに送出する処理を行い、はじめのステップ５０２に飛ぶ（ステップ５１２）。

【００４２】次に、前述した警告メッセージ作成ステップ５０６で作成する警告メッセージの内容とそのＷＢ１００とＰＣ１０１やＭＴ１０２間の警告メッセージ通信プロトコルについて図６を用いて説明する。

【００４３】図６（ａ）でプロトコルシーケンスについて説明する。本プロトコルは最も単純なプロトコルであり、ＷＢ１００から警告メッセージ６００のインディケーションで通知するプロトコルであり、ＰＣからの問い合わせ等は行わないプロトコルである。したがって、送信側はメッセージを送るだけでプロトコル処理を終了する。これに対して受信側では、常にメッセージを受信できるような状態で待機している。これから、警告メッセージ６００の内容について図６（ｂ）を用いて詳述する。警告メッセージ６００は、プロトコルＩＤ６０１、長さ６０２、警告内容６０３、フィルタードフレーム６０４の各フィールドから構成される。プロトコルＩＤ６０１は、本メッセージの正当性をチェックするための特定の識別情報が記載される。長さ６０２は、警告内容６０３の長さを示す。警告内容６０３は、どのＭＢ１００で何時、どのようなウイルスが検出されたかを示す情報が記載される。フィルタードフレーム６０４には、ウイルスが検出されたフレーム自身がきさいされる。これによりウイルスフレームは本警告メッセージにラッピングされて送られる。

【００４４】さて、次にＰＣ１００のハードウェア構成について図９を用いて説明する。

【００４５】９００は、ＣＰＵであり、本装置の中核を成すプログラムの処理装置である。ＣＰＵ９００は、ＣＰＵバス９１０を介して記憶装置であるＲＡＭ３０１やＲＯＭ３０２らとＩ／Ｏ制御装置であるＥterNet制御３０３やＳＣＳＩ制御９０５や画面制御９０８らとインタフェースしている。また、このバスのインタフェース制御はバス制御９０４が制御する。ＳＣＳＩ制御９０５の先には、大容量の記憶装置であるハードディスク装置（ｈｄと略称）９０６やＣＤ－ＲＯＭ装置（ＣＤＲと略称）９０７が接続される。また画面制御９０８の先には表示装置であるＤＩＳＰＡＬＹ９０９が接続する。

【００４６】次に、ＭＴ１０２のハードウェア構造も同様であるが、３０３の代わりに図３での３０４，３０５，３０６，３０７の無線ＬＡＮ用の制御装置が付き、アンテナ３２１に接続される点が異なっている。

【００４７】次に、ＰＣ１０１のソフトウェア構造について図８を用いて説明する。

【００４８】８００ａｂは、ネットワークを使用して他のＯＣ１０１やＭＴ１０２等の計算機と通信する電子メール等の各種アプリケーションプログラム（ＡＰと略称）である。８０４は、ＯＳカネールであり本計算機の種々のリソース（メモリ、プロセス、Ｉ／Ｏ）を制御するプログラムである。８０３はＬＡＮドライバであり、ＬＡＮとのデータのアクセスを制御する。８０２は、通信プロトコル処理でありネットワーク上のデータ転送を保証するプログラムである。８０１は、セキュリティ管理プログラムであり、ＷＢ１００からの警告メッセージを受け取り、ユーザにたいして警告を通知するプログラムである。

【００４９】つぎにこのセキュリティ管理プログラム８０１の処理フローについて図７を使用して説明する。

【００５０】まず最初のステップは、メッセージ受信待ちステップ（ステップ７００）である。メッセージを受信したら次のステップを実行する。次は、当該ＡＰの検出ステップである。これは、受信メッセージに記述された内容からウイルス入りのフレームを受信しようとしてたＡＰを特定する（ステップ７０２）。次に当該ＡＰがコネクションをはっているならば、これを切断する（ステップ７０４）。次に当該ＡＰが開いたままにしていたファイルがあればこれをクローズする（ステップ７０６）。次に当該プロセスを強制終了する（ステップ７０８）。次にウイルス入りのデータを受け取ろうとして強制終了した事をユーザに伝えるためレポートを作成したのちこれを画面に出力する（ステップ７０８）。

【００５１】ＭＴ１０２でもソフトウェア構成は、ＰＣ１０１と同様なので詳細を省略する。

【００５２】次に、ウインドによるＧＵＩ（グラフィカルユーザインタフェース）を備えたＰＣにおけるステップ７０８で画面に出力されるレポートについて図１０を用いて説明する。

【００５３】１００１は、セキュリティ管理メッセージウインドであり、当該ＡＰの強制終了とともに本ウインドが生成される。１００２は、１００１内に表示されるレポートの内容である。これは、以下の各情報を出力表示する。ＡＰ名称として、強制終了されたＡＰの実行ファイル名。ＡＰログとして当該ＡＰが起動された時刻と強制終了させられた時刻、ＡＰ情報として通信相手に関する情報（ネットワークアドレス等）や強制クローズされたファイル名称等を表示する。１００３は、本ウインド制御ボタンであり、これが選択されると本ウインド１００１が閉じられる。１００４は、他のＡＰの実行ウインドである。

【００５４】ＭＴ１０２におけるレポート出力も同様である。ただその内容がウイルス情報をネットワークに流そうとした事を警告するものであることが受信側のＰＣ

と異なる点である。

【００５５】次に、ウイルスチェックモジュール４０１とステップ５０４のウイルスフレームチェック処理ステップの詳細について図１２，１１を用いて説明する。

【００５６】図１２における１２０は、ウイルスコードシグネチャリストであり、ウイルスの名称と当該ウイルスを識別するための特徴であるウイルスのコードの並びとから構成されている。

【００５７】ネットワーク上を流れるフレームのデータは、圧縮されていたり、暗号化されている場合もある。このときは、シグネチャリストには、ウイルスコードの圧縮後のビット列や暗号化後のビット列をシグネチャとして登録しておく。

【００５８】図１１のステップ１１００は、上記リスト１２０の第一コラムのコードを取り出し、検査対象のフレーム内容を先頭から順次ウイルスコードと比較し一致していないかチェックする（ステップ１１００）。一致していれば図５で示したステップ５０８に進む。次は、終了判定ステップである。検査フレームの最後に達してかつリスト１２０の最終コラムに記されたウイルスコードの比較が終了したかどうかを調べる（ステップ１１０２）。その結果終了したならばステップ５１０に飛ぶ。そうでなければ、リスト１２０の次のコラムのウイルスコードを比較のための内容として取り出す（ステップ１１０４）。次に最初のステップ１１００から繰り返す。

【００５９】このようにして、ネットワークのフレームに含まれるコンピュータウイルスを検出し、当該計算機（送り側と受け側双方）にたいして注意を促す事ができる。

【００６０】実施例２

上記例では、警告メッセージ６００にウイルスコードを含むフレームを包みこんで相手に渡していたが、例えば、悪意のあるユーザが本警告メッセージ６００をネットワークから盗み見て既知のウイルスコードを入手し、新しいウイルスを開発しようとすることが有り得る。これを防止することで、より安全性を高めることができる。このために、ウイルスコードを含む警告メッセージを暗号化の手法により分からなくしておく。または、警告メッセージ６００にはウイルスコードを付加せず、警告内容６０３にウイルスが検出されたフレームのヘッダ情報のみを付加する方法でもよい。

【００６１】また、一般のユーザにたいしては、ウイルスフレームをシャットアウトし、ネットワークのセキュリティ管理者（検出ウイルスの解析やワクチン作成のために当該ウイルスを必要とする人）にたいしてのみ、ウイルスコードを含むフレームを前記カプセル化手法を用いて渡すようにしてもよい。このとき、ウイルスフィルタ機能を備えたＷＢ１００等の中継装置において、ネットワークセキュリティ管理者あてにカプセル化されたウイルス入りフレームをきちんと中継するためには、セキュリティ管理社宛のフレームについては、ウイルスフィルタをしない事が必要である。このためには、ウイルスフィルタ機能を備えた中継装置にセキュリティ管理者アドレスを登録しておく。そして図５で説明するとウイルスフレームチェック処理（ステップ５０４）の前に、フレームの宛先アドレスをチェックする処理ステップを追加し、登録された前記アドレス宛であればステップ５０４を実行しないで中継処理ステップ５１０に飛ぶことように変更した処理ロジックで実現される。

【００６２】実施例３

上記実施例では、無線ＬＡＮと有線ＬＡＮとの仲介装置である無線ブリッジであるＷＢ１００にウイルスフィルタ機能を備えた例で説明したが、本発明の方法は、ＬＡＮとＬＡＮとの連結装置であるルータ１０３上においてもＷＢ１００で説明したのと同様な方法でウイルスフィルタ機能を容易に実現できる。

【００６３】さて、以上では無線から有線側に進入することを防ぐ場合のシステムの構成や処理装置について述べてきた。逆の場合、即ち、有線側から無線側にウイルスが出ていくケースのウイルスフィルタ機能も前述した方法により実現できる。

【００６４】実施例４

次は、同一セル１０４内に存在するＭＴ１０２からＭＴ１０２へウイルス入りのフレームが送られるケースでのウイルス侵入対策について図１３を用いて述べる。本ケースでは、対等分散型の無線ＬＡＮを想定しているので、ＷＢ１００は、当該セル１０４の内を飛び交っているフレームをモニタできる。しかし、ＷＢ１００は、セル内のＭＴ１０２間通信でフレーム中継処理をしているわけでないので、実施例１で述べたようなウイルスフレームのフィルタリングは実行できない。なお、集中方式の無線ＬＡＮならば、ＷＢ１００において中継処理を行っているため、実施例１と同様なウイルスフィルタリング機能をＷＢ１００で実現できる。

【００６５】さて、対等分散型無線ＬＡＮにおけるＷＢ１００では、無線フレームを常時モニタしている（ステップ１３００）。ここで、ウイルス入りのフレーム１３１を発信したＭＴ１０２があると、実施例１と同様の方法でウイルスフレームを検出する（ステップ１３０２）。その後警告メッセージをウイルスフレーム受信ＭＴ１０２宛に送り出す（ステップ１３０４）。しかし、これを受け取ったＭＴ１０２は、実施例１で述べたＰＣ１０１のケースと異なりウイルス入りのフレームを既に受信してしまっている。即ち、あるＭＴ１０２がフレームの受信処理を実行している（ステップ１３１０）。ここで、ウイルスフレーム１３１が送られたとすると、その受信完了処理を実行してしまう（ステップ１３１２）。そのため、警告メッセージを受信する前には、ＭＴ１０２におけるウイルスフレームを受信したＡＰが既に終了している事も有り得る。例えば、ユーザ１３０が

ＭＴ１０２内に作成されたウイルス入りの実行ファイルをアクセスし（ステップ１３３０）、その結果システム内にウイルスが感染してしまっているケースも有り得る（ステップ１３１４）。その他、最悪のケースでは、さらに他のＭＴ１０２へウイルスを感染させてしまった後のケースも有り得る。この後、警告メッセージを受けたＭＴ１０２は、警告を表示する（ステップ１３１６）。したがって、ユーザ責任において、ウイルスに汚染された可能性のあるファイルをきり分けて削除するなり、ワクチンプログラム走らせて寄生しているかもしれないウイルスを退治する必要がある。もちろん、ここでは、ワクチンプログラムの起動等は、警告メッセージ表示と連携させて実行する。この場合は、ＷＢ１００がウイルスのタイプを識別し、それに対応するワクチンソフトをメッセージ６００の内容としてＭＴ１０２に通知し（ステップ１３０６）、警告メッセージ６００をうけたＭＴ１０２は、警告メッセージ表示の後、ワクチンを受信し、受信したワクチンの実行確認をユーザにたいして求める（ステップ１３１８）。ユーザがワクチンソフトの起動を指示する（ステップ１３３２）。すると当該ワクチンソフトが実行される（ステップ１３２０）。こうしてウイルスが退治される。ここでは、ワクチンソフトは、ＭＴ１０２にストックして置く方式で説明したが、ワクチンをＭＴ１０２がストックしておき、ＷＢ１００からの警告メッセージにどのワクチンを使用すべきかを通知する方式でも、前記メッセージとともにワクチンを送付する方式でも実現できる。

【００６６】先に述べた最悪のケースで二次感染した場合でも同様に、ＷＢ１００が常時モニタしており、ウイルスフレーム発見時には、警告メッセージを受信ＭＴ１０２に送るのでウイルスへの対応がなされる。したがって、警告メッセージ受信前にＭＴ１０２がパワーオフしたり他のセルに移動したりして、メッセージを受信できないケースを除けば、当該セル内でウイルス感染は収束する。

【００６７】実施例５

また、上記のウイルスフレーム受信ＭＴ１０２に対してのみ警告メッセージを送るのではなく、ＷＢ１００がウイルスをモニタした時点で注意メッセージを当該セル内にブロードキャストし、セル内のすべてのＭＴ１０２に対して注意を促してもよい。これによると二次感染する割合が減少し、すばやく感染がウイルス感染が収束する。

【００６８】実施例６

これから、ウイルスを保有したＭＴ１０２ｃがセル１０４間を移動するケースでの無線ネットワークシステムにおけるウイルス侵入対策の実施例を説明する。

【００６９】ウイルスを保有したＭＴ１０２ｃと通信するＭＴ１０２ｂが同一セル１０４ａ内にあるとき、ＭＴ１０２ｂがウイルスフレーム受信前に他セル１０４ｂに

移動する場合は、ＷＢ１００のウイルスフィルタ機能により対応される。そこで、ウイルス保有ＭＴ１０２ｃが他セル１０４ｂに移動するケースを例にして発明の詳細を説明する。

【００７０】図１４，１５は、本実施例におけるＷＢ１００の警告メッセージ配布処理フローチャートであり、図１４は、ウイルスフレーム検出後の警告メッセージ発行処理であり、図１５は、他のＷＢ１００から警告メッセージを受信後のメッセージ配布処理である。

【００７１】まず、ＷＢ１００は、フレームをモニタし、そこにウイルスが入っていないか検査する（ステップ１４００）。そして、ウイルスを検出したら次のステップを実行する。次は、フレームのヘッダからその送り元であるウイルス保有ＭＴのアドレスを記憶する（ステップ１４０２）。次に、ウイルス保有ＭＴには、ウイルス送出違反の警告メッセージを、ウイルスフレーム受信者には、ウイルスフレーム受信の警告メッセージを、そして、残る同一セル内のＭＴ１０２に対してウイルスフレーム検出の警告メッセージを通知する（ステップ１４０４）。同一のＬＡＮ内の各ＷＢ１００に対してマルチキャストでウイルス保有ＭＴ検出警告メッセージを通知。このとき、メッセージ中に参照カウントをセットしてメッセージを送り出す。また、各ＷＢは、隣接する（ルータの先に接続した）ＬＡＮにおける代表Ｗｂのアドレスを知っている。そして、ウイルスフレーム検出ＷＢは、マルチキャスト範囲外の隣接するＬＡＮの代表ＷＢに対しても警告メッセージを通知（ステップ１４０６）。

【００７２】次に図１５にて、ステップ１４０６で発行された警告フレームを受けたＷＢの処理を説明する。まず、警告メッセージを受信して、自分が代表ＷＢであるかないかによって処理ケースを振り分ける（ステップ１５００）。そして代表ならば、当該ＬＡＮ内の他のＷＢ１００に配布するため警告メッセージをマルチキャストし、そして警告メッセージ中の参照カウントを減算して０かどうかをチェックする（ステップ１５０２）。そしてこの結果が、０ならば、これ以上隣接のＷＢ１００に配布しない、そうでなければ送り元を除く隣接する代表ＷＢに対して警告メッセージを通知する（ステップ１５０４）。いずれのケースでも最後は、受け持ちセル内の全ＭＴに警告メッセージを同報（ステップ１５０６）する。

【００７３】なお、ＷＢからＷＢへの警告メッセージの参照カウントは、検出されたウイルス保有ＭＴの移動範囲が大きいものを程大きくすると効果的に配布される。

【００７４】上記警告メッセージにはウイルスＭＴを検出したＷＢ１００のアドレスが記述されており、ウイルスが検出されたセルの位置がわかるようになっている。上記警告を受け取った各ＷＢにおいてウイルスが検出されたセルに近いものは、当該セル内の各ＭＴ１０２にウ

イルス保有ＭＴを伝え、このＭＴ１０２と通信するときは注意するように伝える。これにより、ウイルスに感染したＭＴ移動してくることによるウイルスの感染に対して、前述の警告メッセージを受信したＭＴ１０２は、必要に応じて備えることができる（当該ＭＴと通信しない等）。また、最悪のケースとして、本警告メッセージ受信の前にウイルス保有ＭＴが移動してきた場合では、各ＷＢ１００でのウイルスフレーム検出・駆除機構に任せられる。また、警告メッセージを受けたＭＴ１０２において、ウイルスが検出されたセルへ移動するものは、ウイルスのトラップを起動しておいてもよい。これにより、汚染セル（ウイルス駆除が完了していない）へ移動した場合での感染を防止する事ができる。

【００７５】次に、図１６を用いて警告メッセーシジを受け取るＭＴの処理フローを説明する。まず警告メッセージの振り分けを行う（ステップ１６００）。ここで、ウイルスを検出したＷＢ１００のアドレスが現在のセルのＷＢ１００と一致していない場合は、異なるセルでウイルスが検出されたと判断して、ステップ１６０２からを実行する。前記判定で、同一の場合はステップ１６１０からを実行する。そして、また、自分がウイルス保有ＭＴであるかを、警告メッセージから識別し、そうである場合はステップ１６０６からを実行する。この処理の詳細では、後で述べる事とし、ここでは、それ以外のケース、即ち、自分がウイルス保有ＭＴでない場合の処理について説明する。まず、他セルのケースから説明する。このケースでは、まず、ウイルス保有ＭＴをウイルス保有者リスト２５０に登録する（ステップ１６０２）。

【００７６】ここで、図２５によりウイルス保有者リスト２５０について説明する。ウイルス保有者リスト２５０は、現在ウイルスを保有しているＭＴの識別情報を記憶したものであり、ＭＴの識別情報が並んだ参照用のテーブルである。図１６に戻り処理フローの続きを説明する。登録ステップ１６０２の後、注意メッセージをＭＴ１０２の画面に表示する（ステップ１６０４）。次に、同一セルのケースを述べる、まず、ステップ１６０２と同様にウイルス保有者リストに登録する（ステップ１６１０）。次に、ＷＢ１００から送られたワクチンプログラムの実行処理を行う（ステップ１６１２）。

【００７７】先に説明したように、警告メッセージを受けた各ＭＴ１０２は、ウイルスフレームを発信したＭＴ１０２と通信する事は控える（原則として行わない）。これを実現する処理フローを図１７で説明する。まず、起動されたＡＰが通信しようとしているかどうかをチェックする（ステップ１７００）。ここで通信要求があれば次の処理を実行しそうでなければ繰り返す。次は、ウイルス保有者リストをチェックし、通信相手が登録されていないかをチェックする（ステップ１７０２）。通信相手が登録されていれば、確信表示ステップ１７０４を

実行し、そうでなければ、通信処理（ステップ１７１４）を実行する。確認表示処理は、ユーザに対してウイルスを保有している相手との通信を望んでいるかを確認する処理ステップである。次にユーザからの応答を受取りこれをチェックする（ステップ１７０６）。この結果ユーザが通信を希望する場合は、ステップ１７０８を実行し、そうでなければ、当該ＡＰを終了し（ステップ１７１０）、はじめのステップに戻る。ステップ１７０８は、通信相手へのウイルス駆除完了の問い合わせを実行し、その応答結果を判定する（ステップ１７０８）。この応答結果が、ウイルス駆除完了ならば、ウイルス保有者リストから通信相手ＭＴを抹消し（ステップ１７１２）、通信処理ステップ１７１４を実行する。応答結果がウイルス駆除未完了ならば、当該ＡＰを終了して（ステップ１７１０）はじめのステップ１７００に戻る。

【００７８】次に、ウイルス入りフレームを発信したＭＴ１０２は、以後他のＭＴ１０２と通信されなくなるため、これを解除する方法を説明する。ウイルスフレームを発信したＭＴ１０２は、ＷＢ１００から警告メッセージを受ける。このケースでは、ステップ１６００が実行されたあと、ステップ１６０６が実行される。まず、自分がウイルスに汚染されているという状態変数をもち、これをセットした後、ＷＢ１００から送られた当該ウイルスのワクチンプログラムを実行する（ステップ１６１６）。次に、これが成功したら、ウイルス駆除完了メッセージを当該ＷＢ１００に報告し、ウイルス汚染状態をリセットして終了する（ステップ１６０８）。

【００７９】次に、このウイルス駆除完了メッセージを受けるＷＢ１００の処理について図１８を用いて説明する。基本ロジックは、図１４で示した警告メッセージと同じ方法でウイルス駆除完了通知を近接するＷＢに通知する。まず、ウイルス駆除完了メッセージを受信する（ステップ１８００）。次に、ウイルス保有者リストから当該ＭＴを削除する（ステップ１８０２）。次に、ステップ１４０４からと同様の方法で警告メッセージを配布した範囲にウイルス駆除完了メッセージを配布する。このメッセージを受けたＷＢ１００の処理は、図１５と同様なので詳細は省略する。ここでは、ＷＢ１００が受け持つセル内の各ＭＴ１０２にウイルスＭＴの登録解除メッセージが送られる。このメッセージを受けたＭＴ１０２は、ウイルス保有者リストから通知されたＭＴ１０２を削除する。

【００８０】先程説明したように、ＭＴ１０２は、ウイルス保有者リスト上の登録されたＭＴ１０２と通信する場合、ウイルス保有ＭＴにウイルス駆除完了問い合わせを行う。図１９で、この問い合わせを受けるウイルス保有ＭＴの処理フローを説明する。まず、自分がウイルス汚染状態かどうかをチェックする（ステップ１９００）。その結果、対応する警告メッセージのウイルス駆除が完了していれば、問い合わせの応答として、駆除完

了メッセージを返送する（ステップ１９０２）。そして、未完了ならば、ウイルス駆除未完了メッセージを返送する（ステップ１９０４）。

【００８１】次に、ウイルスＭＴへの警告メッセージの表示内容について補足説明をする。前述したようにワクチンプログラムが送られた後、ワクチンプログラムを実行するので、メッセージとして、「ウイルス退治中です、しばらくこのままでお待ちください、電源切断や、移動することは控えてください」とのメッセージをワクチンプログラムが終了するまで表示しておく。

【００８２】実施例７

以上の実施例は、既知のコンピュータウイルスに対抗するコンピュータネットワークシステムを示した。それは、ＷＢ１００が中核となってウイルスチェック機能を行う実施例であり、主として次のようなケースに適応した物である。具体ケースとして、例えば、不特定多数がアクセスしセキュリティの管理がしっかりできないコンピュータネットワークでは既知のウイルスが潜伏している可能性がある。そのようなコンピュータネットワークにＭＴ１０２が移動し、そこで情報を入手したときにウイルスに感染する可能性がある。そのご、ウイルスに感染したＭＴ１０２が、セキュリティや信頼性が要求されるネットワークに戻ってきたときに、当該ネットワークの基幹部に既知のウイルスが進入するのを防ぐ場合である。

【００８３】ここでは、未知のウイルスに対応するコンピュータネットワークシステムの実施例を説明する。これは、どのようなケースに対応するかというと、例えば、信頼性の保証できないネットワークで悪質なユーザが新しいウイルスを開発してばらまく、たまたま、このようなネットワークに接続したため、未知のウイルスに感染したＭＴ１０２が信頼性の要求されるネットワークに戻ってくる場合や悪質なハッカーや害意のあるユーザが直接無線ネットワークから新ウイルスを散布するケースに対応する発明である。

【００８４】まず、ＷＢ１００への付加機能について説明する。未知の新ウイルスは既知ウイルスの基本コードからの派生物と考えられる。そこで、ＷＢ１００のウイルスチェック処理にＡＩ手法を取り入れることにより、実施例１で示したフレーム内容とウイルスコードとの一致・不一致のみで判定するのではなく、ファジー推論により、ウイルスコードとの類似度を評価して、その評価値が或一定値以上ならば、未知のウイルスの可能性があると判断する機能を付加する。このようなＷＢ１００の処理フローを図５と図２０を用いて説明する。なお、この図２０は、図５からの追加・変更部を説明する。まず、ステップ５０２の受信フレーム待ちのあと、ステップ５０４の変わりに上述した方法で当該フレームにおけるウイルスの含有推定率を求め、この値によって次の３つの処理ルートに振り分ける（ステップ２０００）。まず第１のルートは、０％に近い或る値以下のケースであり、この場合は、ウイルスが含まれていないと判断して、ステップ５１０の中継処理に飛ぶ。第２のルートは、１００％に近い或る値以上のケースであり、この場合は、ウイルスが含まれていると判定して、ステップ５０６の警告メッセージ作成処理に飛ぶ。第３のルートは、前記以外の値のケースであり、未知のウイルスが入っているかもしれないと判断して次のステップに進む。次のステップは、ウイルス入りのフレームかも知れないという意味の容疑メッセージを当該端末に対して送る（ステップ２００２）。そして次にステップ５１０の中継処理から実行する。

【００８５】次に、ＰＣ１０１の付加機能について図２１を用いて説明する。まず、ＰＣは、上記警告メッセージを受信する（ステップ２１００）。次に、当該フレームを受信したＡＰを探し出し、それが書き込みモードでアクセスしたファイル一覧を検索し記憶する（ステップ２１０２）。次に、ウイルスが進入したかもしれないという警告表示をユーザにたいして提示し、合わせて、当該ＡＰの終了を促す（ステップ２１０４）。そして、当該ＡＰの終了を待つ（ステップ２１０６）。次に、ステップ２１００２で記憶したファイルをアクセス禁止モードにする（ステップ２１０８）。その後、後で詳細を説明するセキュリティサーバに対して未知のウイルスが進入した可能性のあるファイルの検査を依頼する（ステップ２１１０）。そして、その応答結果を受信するまで待つ（ステップ２１１２）。次に、その応答結果をチェックする（ステップ２１１４）。そして異常なしならば、当該ファイルアクセス禁止モードを解除して、ユーザＡＰによるアクセスができるようにする（ステップ２１１６）。異常ありと判断されたならば、当該ファイルを削除する（ステップ２１１８）。

【００８６】次は、セキュリティサーバを図２２を用いて説明する。２２００はセキュリティサーバであり、ハードウェア・ソフトウェアともに基本はＰＣ１０１と同一であるため、付加機能ブロックを図で表示している。２２０１は、以来受け付け、結果送信ブロックであり、ここで、ＰＣ１０１からの検査を依頼されたファイルを受け付け、またその検査結果をＰＣ１０１に対して送信する。以下の機能ブロックで実現される依頼ファイルのシミュレート実行で異常を検出しなければ、ファイル検査依頼のあったＰＣ１０１に異常なしとの応答を返し、そうでなければ、異常ありとの応答を返す。２２０２は、依頼環境構築部であり、依頼のあったＰＣのダミーの動作環境を構築する機能ブロックである。２２０３は、依頼されたファイルのテスト実行の結果、異常が起こらないか監視し、これを検出する機能ブロックである。ここには、ウイルスが原因となる異常を検出する機構、具体的には、ファイルサイズの増分チェックやメモリスキャンチェックによるウイルス寄生部の摘発機能等

を備えている。２２０４は、依頼ファイルのエミュレート実行部であり、２２０２で設定された動作環境で、時刻タイマーのアップや当該ファイルの複数回実行をシミュレートする機能ブロックである。以上の機能ブロックを備えた計算機がセキュリティサーバである。

【００８７】以上は、ウイルス検査機能をセキュリティサーバというネットワーク上の専用計算機にで実現する例を説明したが、高速のＣＰＵや大規模なメモリを持つ事でＷＢ１００においてもその中継性能を低下させることなく実現する事ができる。

【００８８】実施例８

次に、前述したセキュリティサーバ２２００で異常のあったファイルから未知のウイルスを抽出し、その識別情報を各ＷＢ１００に通知することで、未知のウイルスを既知の物としてＷＢに自動登録する機構を図２３を持ちいて説明する。

【００８９】このとき、セキュリティサーバは２２００は新規ウイルス登録メッセージを各ＷＢ１００宛にマルチキャストする。図１４と図１５で説明したのと同様な方法で代表Ｗｂが隣接ネットの代表Ｗｂにウイルス登録メッセージを通知する事でネットワーク全体に配布される。

【００９０】一方のＷＢでは、新規ウイルス登録メッセージを受信する（ステップ２３００）。次に、ウイルスコードシグネチャリストに前記メッセージの内容を登録する（ステップ２３０２）。このようにして、以後登録されたウイルスを含むフレームは、ＷＢ１００でフィルタリングされる事になる。無論ここで、新規ウイルス登録メッセージに記述されたウイルスコードは、前にウイルスフレームのカプセル化手法で述べたようにＷＢにおけるウイルスフレームのフィルタリング例外とする。

【００９１】なお、セキュリティサーバ２２００が発見した未知のウイルスに対するワクチンソフトを作成し、これを新規ウイルス登録メッセージに付加する事で各ＷＢ１００に配布してよい。

【００９２】その他、ワクチンソフトが格納されたセキュリティサーバ２２００のアドレスを新規ウイルス登録メッセージを受けたＷＢ１００に登録させておき、その後、前記メッセージによって登録されたウイルスの警告メッセージをＰＣ１０１やＭＴ１０２に送る。ＷＢ１００は、前記ＰＣ１０１やＭＴ１０２からの問い合わせに応じてワクチンを保有するＳＳのアドレスを通知する。そして、このアドレス通知を受けたＰＣ１０１やＭＴ１０２が当該セキュリティサーバから当該ウイルスのワクチンをロードする方法でもよい。これでＰＣ１０１やＭＴ１０２における未知ウイルスにたいする対応がなされる。

【００９３】実施例９

前述の例では、セキュリティサーバ２２００が新規ウイルス登録メッセージをマルチキャストで各ＷＢに配布すると説明したが、隣接するＷＢ１００間で定期的にウイルスシグネチャコードリスト１２０の新規追加部分を教え合い、自分に足りない物が隣接ＷＢにあったらそれを取得するという方法でも配布できる。これは、ネットワークの事故や当該Ｗｂの電源ｏｆｆ等により新規ウイルス登録メッセージを受け取れなかったＷｂ１００が存在した場合に有効な方式である。この処理方法について図２４で説明する。処理フロー２４００は、通知処理フローである。まず、タイマを起動し一定時間に達するまで待つ（ステップ２４０２）。次に、テーブル１２０で新規に追加した物を選びだしこれを追加リストに編集して隣接するＷＢ１００に通知する（ステップ２４０４）。ここで新規追加分を選び出すために、追加した物はその追加時刻を記述しておき、現在の時刻と追加時刻を比較し一定範囲内の物を選びだすようにする。２４１０は、登録処理の処理フローである。

【００９４】まず、通知された追加リストを受取り、その内容をみて、現在テーブル１２０に登録されていない物が存在するかどうかをチェックする（ステップ２４１４）。登録すべき物があるならテーブル１２０に登録する（ステップ２４１４）。以上で処理を終了する。

【００９５】以上実施例のように構成すれば、以下の効果がある。

【００９６】１．まず、はじめに、実施例のように構成すれば、コンピュータネットワークシステムへのコンピュータウイルスの進入を防止できる。つまり、不特定多数のコンピュータが接続しウイルスが進入する可能性があるようなセキュリティ面で不安があるが、しかし、リアルタイムで有用な情報をアクセスできるようなネットワーク、例えば、インターネットと、従来から存在するセキュリティレベルの高い企業内ネットワークとをセキュリティレベルを損なうことなく接続できる。その結果、オープン化に対応したネットワークシステムを構築する事ができ、その結果、有効な情報を安全に入手できるという効果がある。

【００９７】また、移動端末が普及した企業内ネットワークにおいて、移動端末が一旦企業内ネットワークから離れて、様々な情報活動を行う。例えば、他の信頼性の無いネットワークにアクセスして情報を入手したり、ＣＤ－ＲＯＭ等の流通メディアをアクセスしたりである。

【００９８】この後、移動端末が再度企業内ネットワークに接続されるケースで、再接続の前に、ウイルスチェックプログラムを起動し、ウイルスに感染していない事を確認しなくても、同程度のセキュリティレベルを維持する事ができる。つまり、再接続時のウイルス駆除処理オーバーヘッドを必要とせず、かつ、セキュリティレベルはそのままで、スムーズに元のネットワークにアクセスできる。また、移動端末では、ウイルスチェックをプログラムを定期的に起動しなくても済むという効果もある。

【００９９】２．また、上記のように構成すれば、ネットワークの中継装置にウイルスフィルタ機能を設けたことにより、各コンピュータにウイルスフィルタ機能を設けなくても済む。これにより、当該ネットワークシステムにウイルスフィルタ機能を追加するためのコストを低減できる。つまり、本中継装置でウイルスに強いネットワークを構成できる。その上、各コンピュータには、ウイルスフレームを扱う処理を組み込まなくて済むため、ウイルスフレーム処理を参照して悪用しようとするユーザを未然に防止するという効果もある。また、ウイルスの侵入ターゲットとなったコンピュータで処理をしないため、安全であり、かつ、このためのオーバーヘッドをコンピュータにかけなくて済むという利点もある。

【０１００】３．また、他の実施例によれば、そのネットワークの構成上理由から先に述べたウイルスフィルタ機能を備える事ができないネットワークシステムにおいて、ネットワークシステムに接続されたコンピュータは、ウイルス入りのデータを受信すると、警告メッセージが送られるため、ネットワーク上からウイルスが進入した事を当該コンピュータで認識できる。その結果、進入したウイルスに対応した処理を行う事ができるため、定期的にウイルスチェックプログラムを走らせずともよくなるという効果がある。また、ウイルス受信後、直ちに、ワクチンプログラムを走らせる事ができ、コンピュータウイルスの二次感染を防止するという効果もある。

【０１０１】４．また、ネットワーク監視装置にウイルス検出機能を持たせたことで、当該装置で集中的に監視することにより、それぞれのコンピュータでウイルス検出をしなくて済むので、ネットワークに接続した各コンピュータへの負担を増大させることなく、ウイルスに対抗するシステムを実現できるという効果がある。

【０１０２】５．警告メッセージを受けたコンピュータにその内容が表示される事で、ウイルスを受信したコンピュータのユーザは、ウイルスを送信したコンピュータを知ることができ、そこから、何をアクセスした結果ウイルスが進入する事になったか、ウイルス侵入原因の解明を行える。また、その後当該コンピュータからのアクセスを控える事により、ウイルスの進入をユーザレベルで抑止できる。ウイルスを送ったコンピュータにも警告メッセージが送られるため、知らないうちに感染していた事が分かり、その時点でワクチンプログラムを実行させる事でウイルスの駆除ができる。

【０１０３】６．また、ウイルスフィルタ機能を備えたネットワークシステムにおいては、ウイルス入りデータは受信できなくなる。このため、前記データを受信しようとしたＡＰは、異常終了する事になる。本発明では、ネットワークの故障による異常終了とネットワークシステムのウイルスからの防衛のためによる異常終了を切り分ける事ができるという効果もある。

【０１０４】７．また、ある特定のネットワーク管理社

宛には、ウイルス入りのデータをフィルタすることなく正常に送る事で、ウイルスの解析や対抗するワクチンの開発に役立てる事ができるという効果もある。

【０１０５】８．また、ネットワーク上を流れるデータが圧縮されていたり、暗号化されていたりしてもウイルスのチェックができるという効果もある。

【０１０６】９．また、他の発明によれば、ウイルス入りのデータを送受したコンピュータに対して、当該ウイルス用のワクチンプログラムがウイルスを検出した時点で送られるため、直ちにウイルスを駆除できるという効果もある。また、コンピュータにはワクチンプログラムを保存しておく必要が無いため、その分の記憶容量が多く使えるメリットもある。

【０１０７】10．モーバイルコンピュータがウイルスを保持していた場合、それを検出したあるネットワーク監視装置が、モーバイルコンピュータの移動先のネットワーク監視装置にメッセージを送る事で、ウイルスに事前にウイルス対策の準備ができる。また、メッセージの配布範囲を限定した事により、ネットワークにかける負担を少なくするという効果もある。

【０１０８】11．モーバイルコンピュータのウイルス駆除処理において、適切なメッセージをユーザを提示することにより、確実にウイルスの駆除を行え、また、ウイルスの拡散を防止するという効果もある。

【０１０９】12．その他の実施例によれば、ウイルスを保持しているコンピュータを知ることができるため、ウイルスを保持しているコンピュータとの通信をしない事で、ウイルス感染の恐れを防ぐという効果がある。

【０１１０】13．また、モーバイルコンピュータにおいては、ウイルスが検出されたエリアが分かるので、そこエリアに移動することを避ける事でウイルスの感染を防止できる。

【０１１１】14．また、他の実施例によれば、ウイルス保持コンピュータをネットワーク監視装置によりウイルス保有コンピュータを一元管理する事で、各コンピュータにおけるウイルス保有コンピュータの一覧を保持しなくて済むという効果がある。

【０１１２】15．また他の実施例によれば、新しいコンピュータウイルスを逸早く検出する事ができるため、当該ネットワークで今までに存在していなかったコンピュータウイルスによる被害を食い止める事ができる。

【０１１３】16．また、ウイルスフィルタ機能を備えたネットワーク中継装置にウイルス推定機能を追加した事で、疑わしいデータフレームにマークを付加する事ができ、当該データを受け取ったコンピュータは前記マークをみる事で容易に疑わしいデータである事を認識できるという効果がある。

【０１１４】17．また、ウイルスが含まれている可能性のあるファイルをリモートにある検査専用コンピュータにその検査を依頼している最中に、その疑わしいファイ

ルのアクセスを禁したため、もし、当該ファイルにウイルスが含まれていた場合に第３のコンピュータへ拡散することを防ぐという効果がある。

【０１１５】18. ウイルス検査専用コンピュータを当該ネットワークシステム内に設ける事で、システムにおける通常処理の能力を低下させることなく、コンピュータウイルスに強いネットワークシステムを構築できるメリットがある。

【０１１６】19. 新規ウイルスの識別情報をウイルスフィルタリング実行機器に配布する事で、以降同一のウイルスは、フィルタリングで落とされるので、コンピュータは、ウイルス検査専用コンピュータに御墨付きをもらう処理しなくても済むという効果がある。

【０１１７】20. ウイルスフィルタリング機能を備えたネットワーク中継機器でウイルスの識別情報を定期的に交換しあうため、当該中継機器が障害等により新しいウイルス識別情報を受信できなかった場合でも、一定時間後には、受信できることが保証されるという効果もある。

【０１１８】21. ウイルスチェック機能を備えたネットワーク監視装置で未知のウイルスを新規ウイルスとして検出できるようになるという効果がある。

【０１１９】22. 上記ネットワーク監視装置に新規ウイルスにたいするワクチンが配布されるため、新規ウイルスを検出したら、対応するワクチンプログラムを関連コンピュータに配布し、これを受信したコンピュータ上で前記の新規ウイルスの駆除ができるという効果がある。

【０１２０】

【発明の効果】以上の説明から明らかなように、本発明によれば、コンピュータウイルスへの耐性が強いコンピュータネットワークシステムを構築することができる。

【図面の簡単な説明】

【図１】本発明の一実施例を示すネットワーク防疫システムの概要構成図である。

【図２】本発明の一実施例を示すコンピュータウイルスフィルタ機能を無線ＬＡＮブリッジで実現したブロック図である。

【図３】図２の無線ＬＡＮブリッジのハードウェア構成例を示す図である。

【図４】図２の無線ＬＡＮブリッジのソフトウェア構成図である。

【図５】図２の無線ＬＡＮブリッジの主要な処理のフローチャート図である。

【図６】図６（ａ）は、無線ＬＡＮブリッジとＰＣとの管理プロトコルシーケンス図であり、図６（ｂ）は、無線ＬＡＮブリッジとＰＣとの管理プロトコルで渡されるメッセージの形式を示す図である。

【図７】ＰＣにおけるセキュリティ管理プログラムの処理フローチャートである。

【図８】ＰＣ上のソフトウェア構成図である。

【図９】ＰＣのハードウェア構成図である。

【図１０】警告メッセージ通知画面の一例を示す図である。

【図１１】ウイルス判定処理の処理フローチャートである。

【図１２】ウイルスコードシグネチャリストの構造を示す図である。

【図１３】警告メッセージのシーケンスを説明する図である。

【図１４】警告メッセージ発行処理の処理フローチャートである。

【図１５】警告メッセージ配布処理の処理フローチャートである。

【図１６】警告メッセージ受信処理の処理フローチャートである。

【図１７】ウイルス保有コンピュータとの通信を控える処理の処理フローチャートである。

【図１８】ウイルス駆除完了受信処理の処理フローチャートである。

【図１９】ウイルス駆除完了問い合わせの受け付け処理の処理フローチャートである。

【図２０】ウイルス推定ロジックを付加したときの処理フローチャートである。

【図２１】ＰＣにおけるウイルス検査依頼処理の処理フローチャートである。

【図２２】セキュリティサーバの説明図である。

【図２３】新規ウイルス登録処理の処理フローチャートである。

【図２４】新規ウイルス情報交換処理の処理フローチャートである。

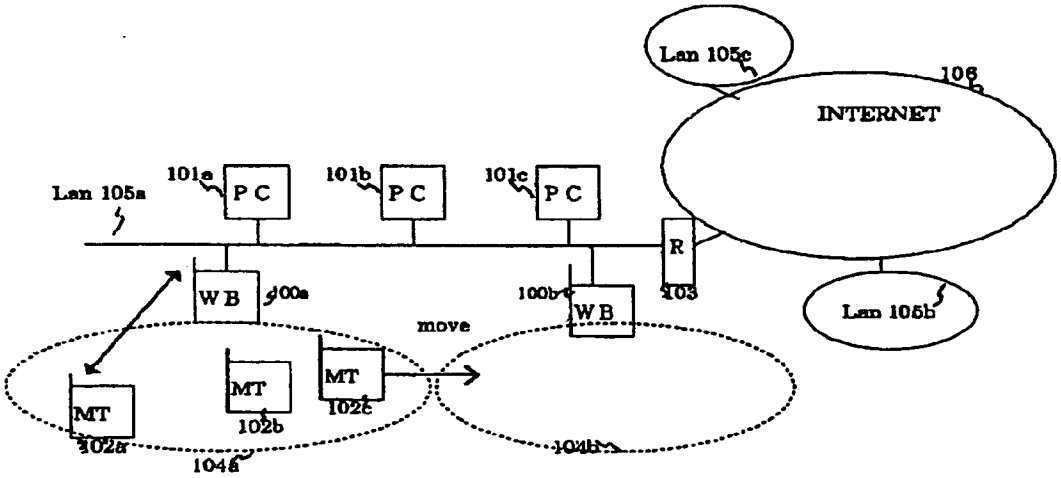
【図２５】ウイルス保有者リストの構造を示した図である。

【符号の説明】

１００…無線ブリッジ、
１０１…パーソナルコンピュータ、
１０２…モーバイルコンピュータ、
１２０…ウイルスコードシグネチャリスト、
２０２…ウイルスチェックブロック、
２０３…警告メッセージフレーム作成ブロック、
２５０…ウイルス保有者リスト、
６００…警告メッセージ、
２２００…セキュリティサーバ。

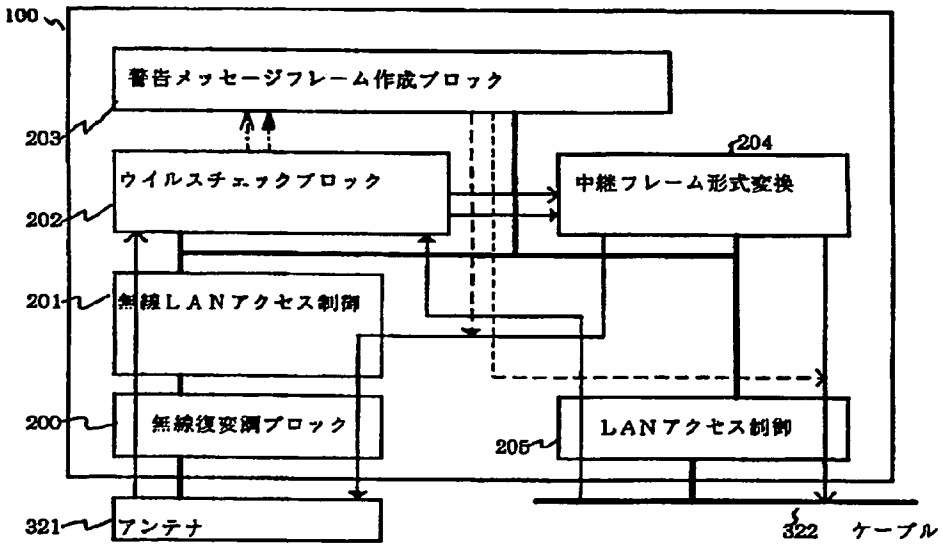
【図１】

図　１



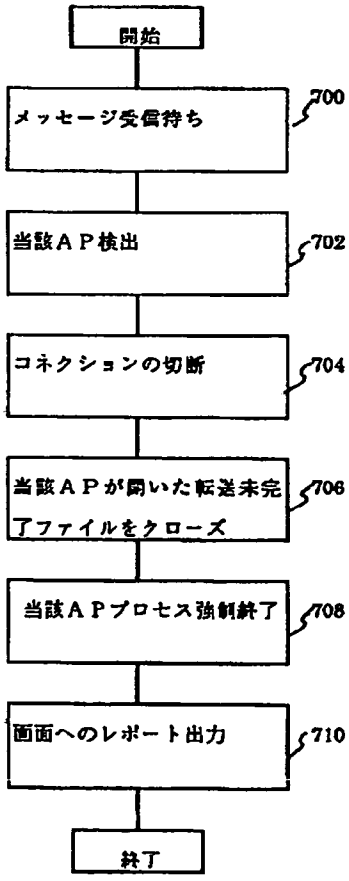
【図２】

図　２



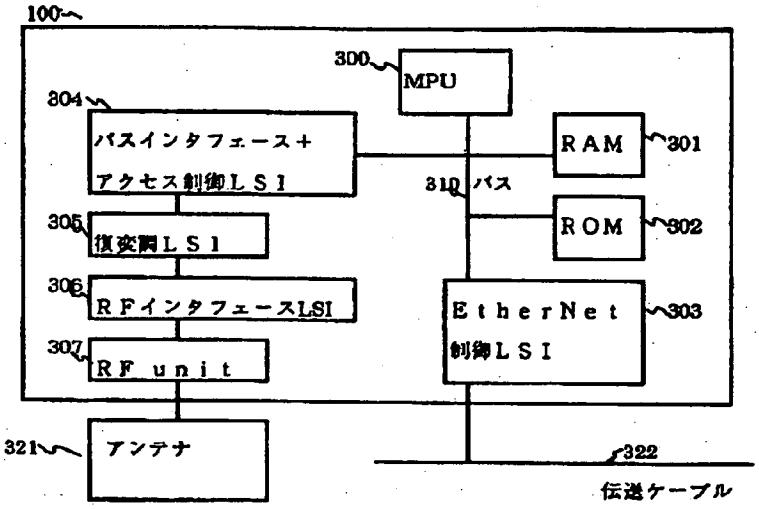
【図７】

図　７



【図３】

図 3



【図１２】

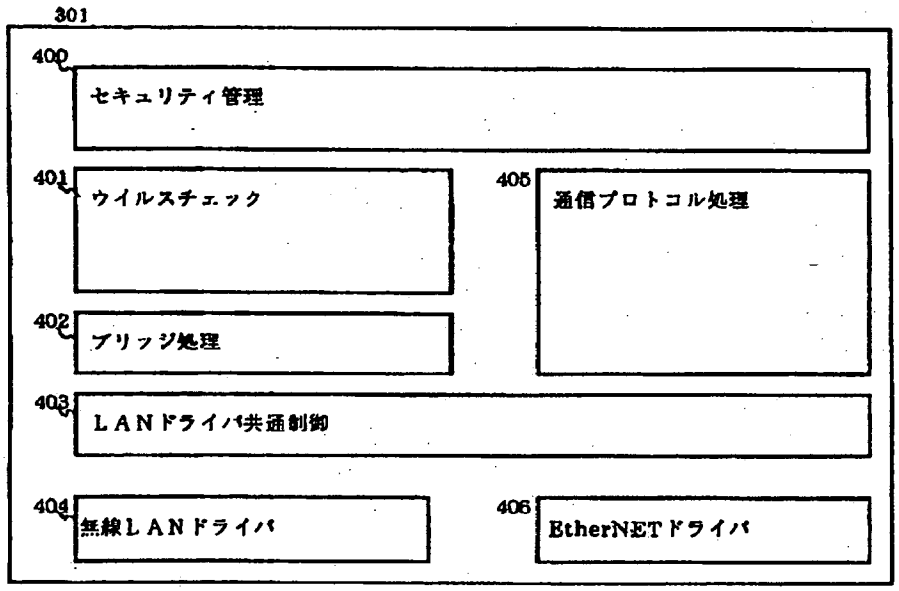
図 12

120

ウイルスコードシグネチャリスト	
名称	コード

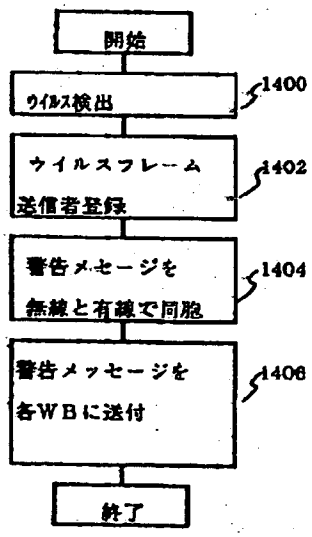
【図４】

図 4



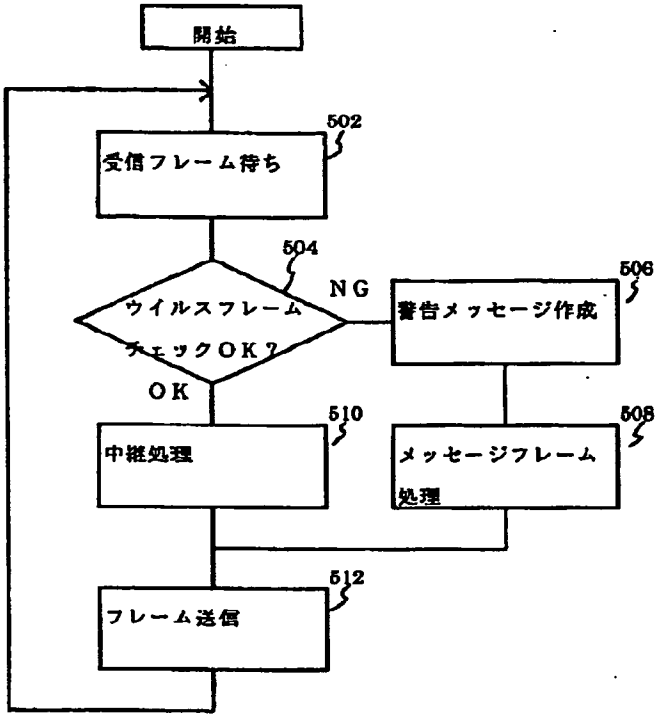
【図１４】

図 14



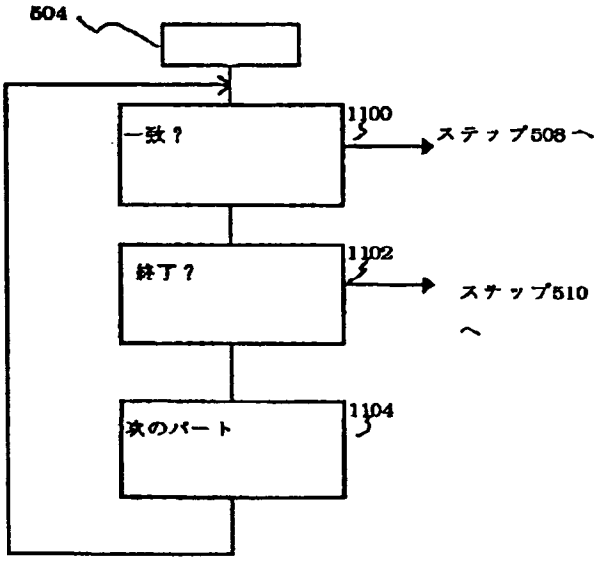
【図5】

図 5



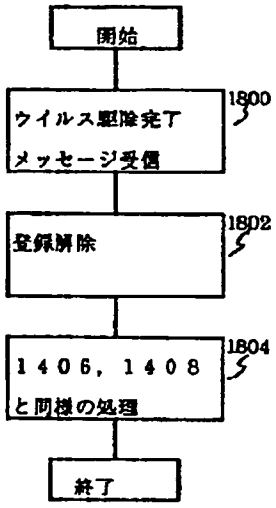
【図11】

図 11



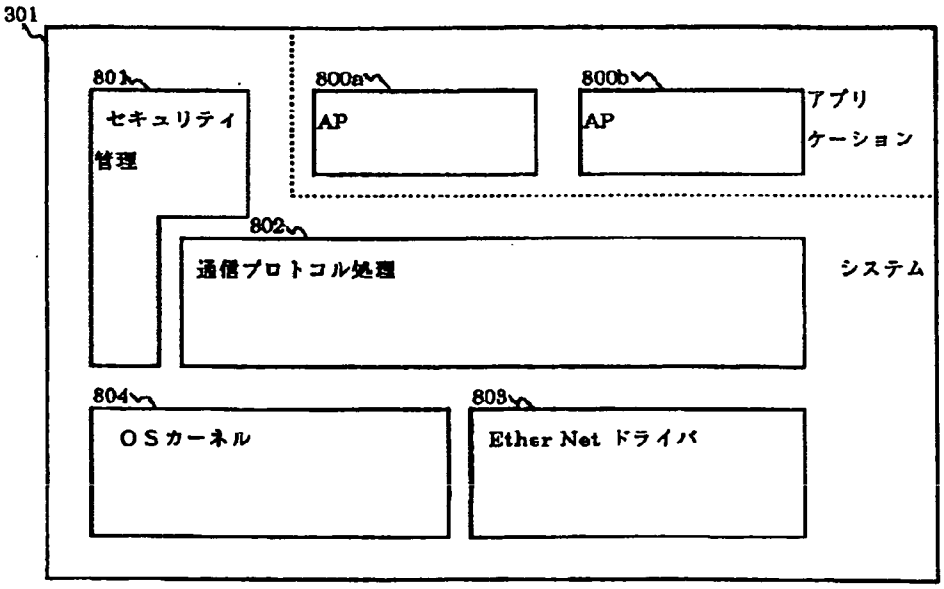
【図18】

図 18



【図8】

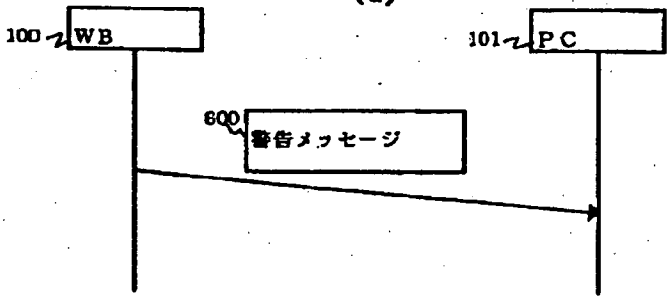
図 8



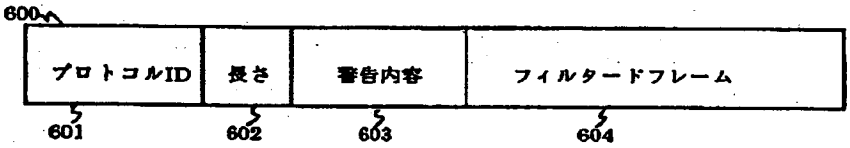
【図６】

図 6

(a)

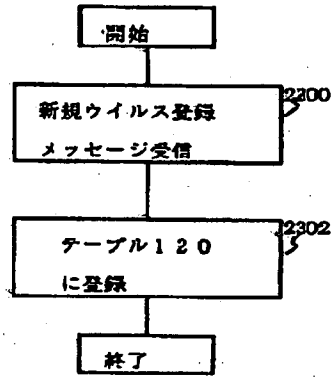


(b)



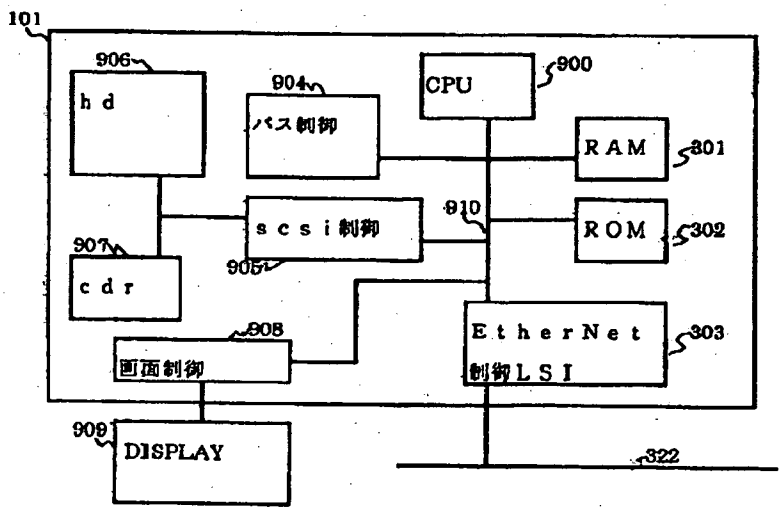
【図２３】

図 23



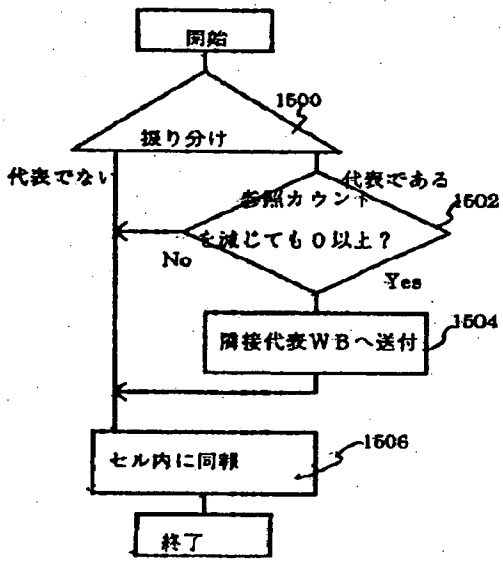
【図９】

図 9



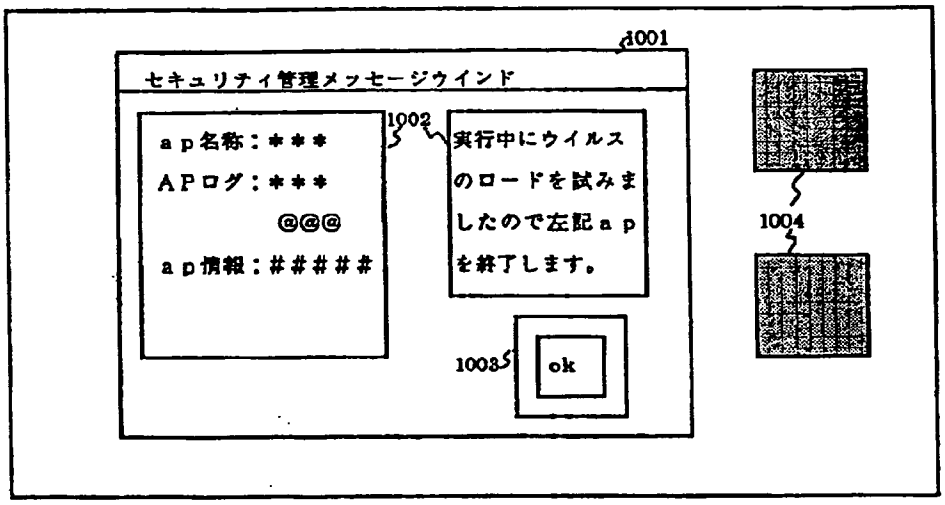
【図１５】

図 15



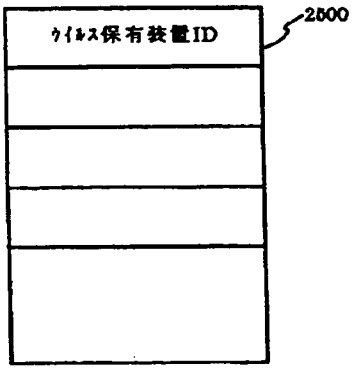
【図１０】

図 10



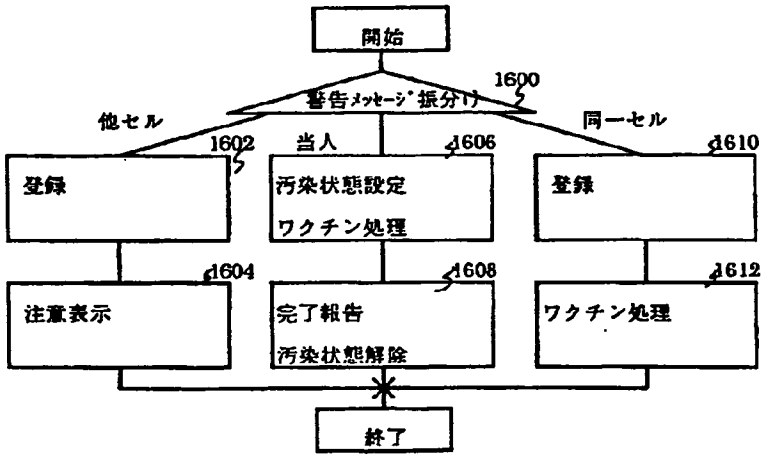
【図２５】

図 25



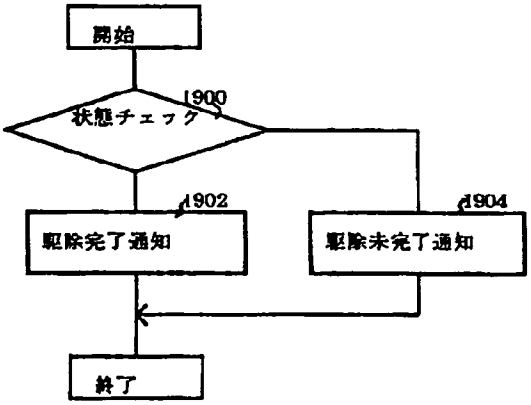
【図１６】

図 16



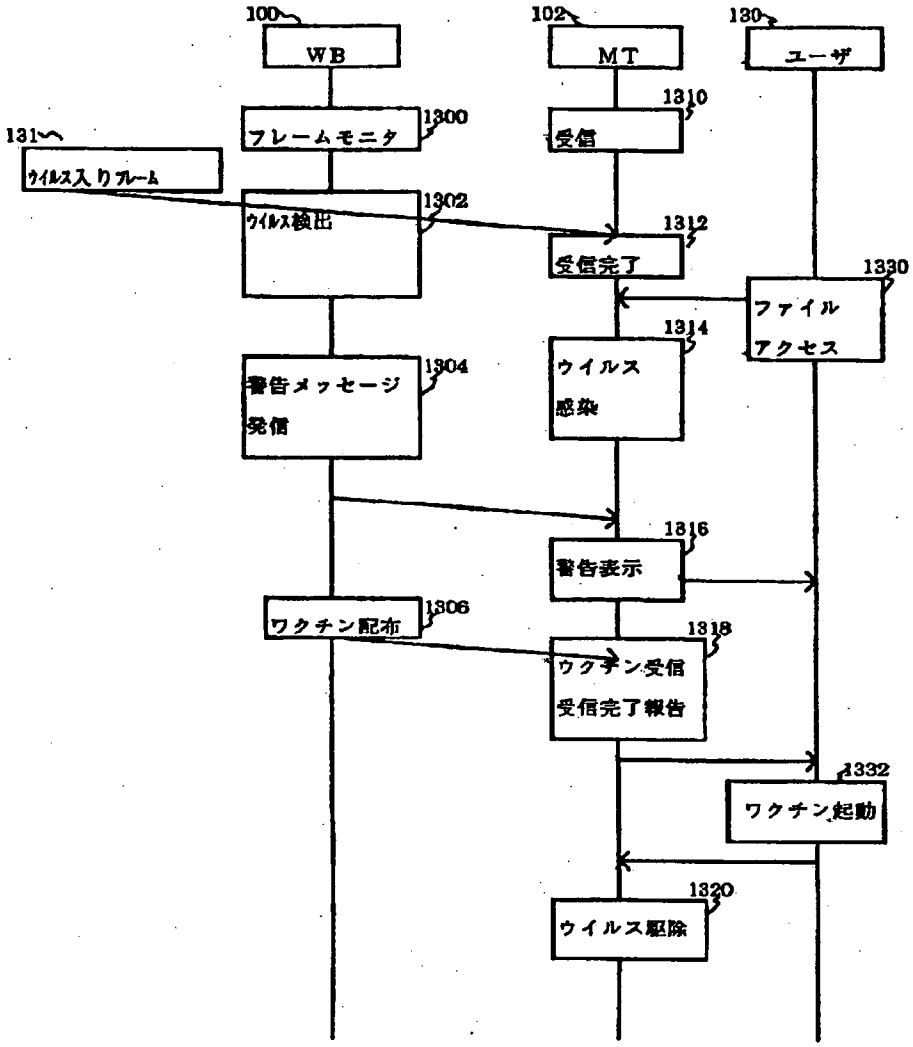
【図１９】

図 19



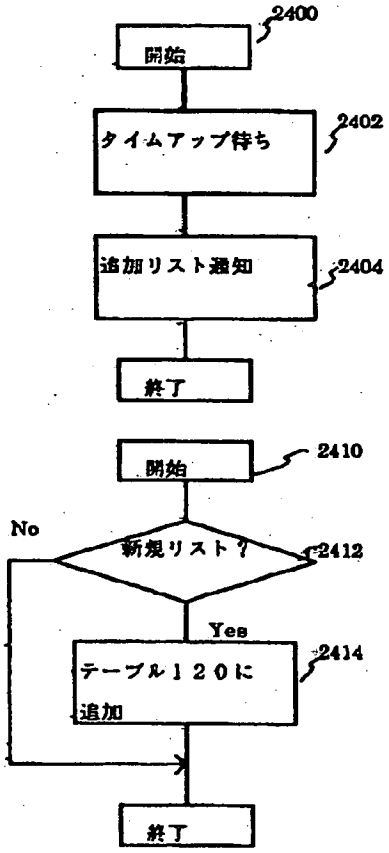
【図１３】

図 13



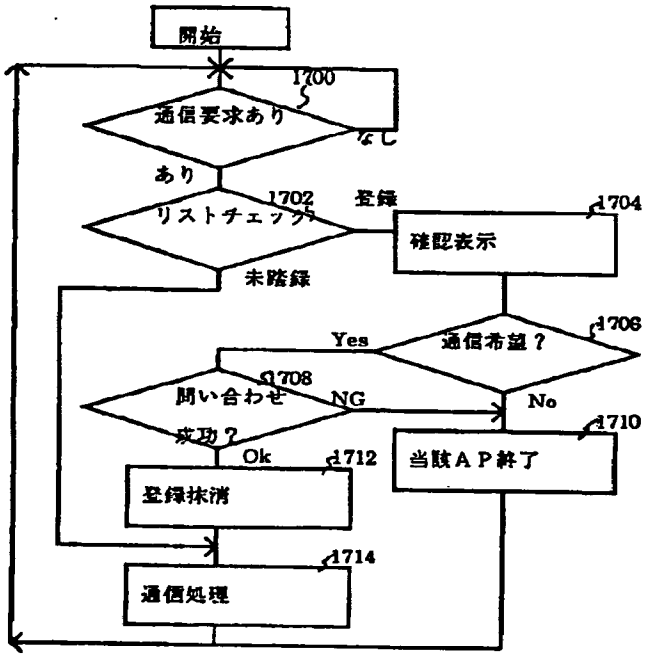
【図２４】

図 24



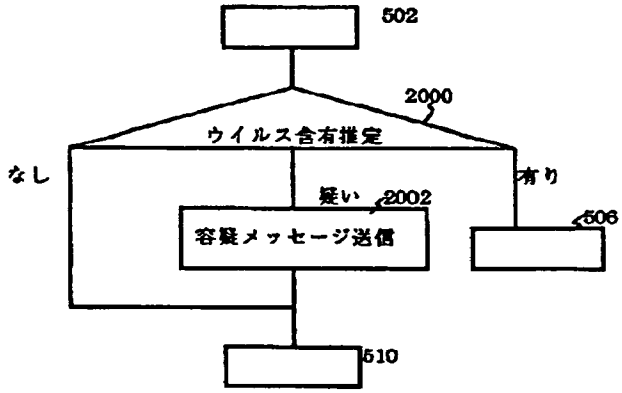
【図１７】

図 17



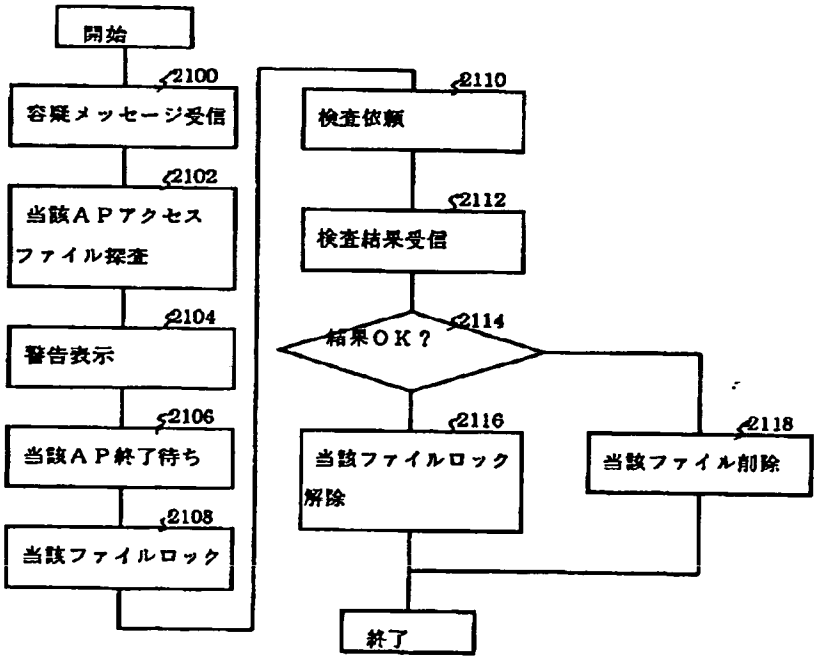
【図２０】

図 20



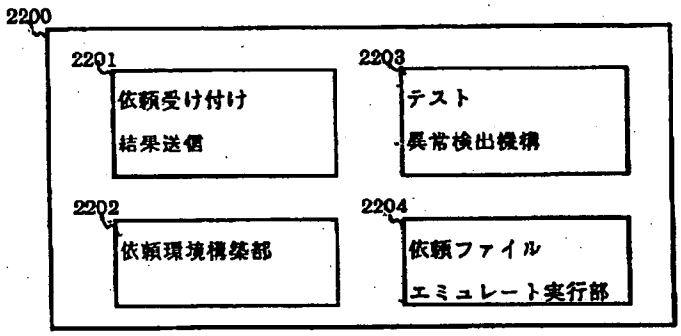
【図２１】

図 21



【図２２】

図 22


2200
2201
依頼受け付け
結果送信
2203
テスト
異常検出機構
2202
依頼環境構築部
2204
依頼ファイル
エミュレート実行部